(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-164553
(P2004-164553A)
(43)公開日　平成16年6月10日(2004.6.10)

(51)Int.Cl.[7]	F I	テーマコード（参考）
G06F 13/00	G06F 13/00 351Z	5B089

審査請求 未請求　請求項の数 23　OL　（全 ~~26~~ 19 頁）

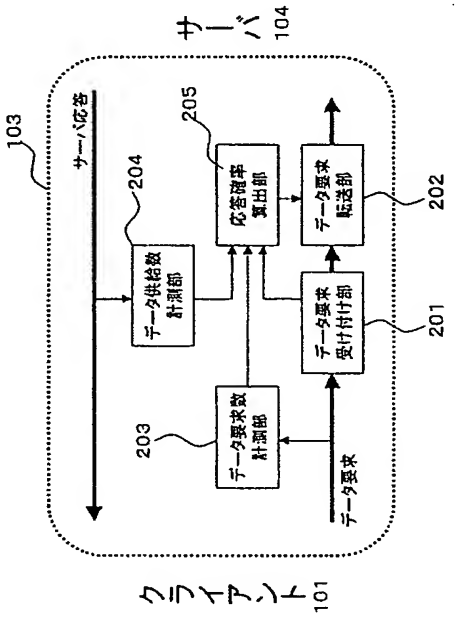
(21)出願番号　特願2003-71238(P2003-71238)
(22)出願日　平成15年3月17日(2003.3.17)
(31)優先権主張番号　特願2002-280289(P2002-280289)
(32)優先日　平成14年9月26日(2002.9.26)
(33)優先権主張国　日本国(JP)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100083161
弁理士　外川　英明
(72)発明者　菅野　伸一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　楯岡　正道
東京都府中市東芝町１番地　株式会社東芝府中事業所内

Fターム(参考)　5B089 GA00 KA17 KB11 KB13 KC29 KC52 MA01 MA07

(54)【発明の名称】サーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機

(57)【要約】
【課題】不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置を提供することを目的とする。
【解決手段】サーバとなる計算機に対してデータ要求される数と、これに応答するサーバのデータ応答の数を用いてサーバ計算機の負荷状態を求め、この負荷状態に応じてサーバに転送するデータ要求の割合を変化させる手段を備えたサーバ計算機保護装置とする。



1

【特許請求の範囲】
【請求項１】
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、
一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、
一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ供給数計測手段と、
前記データ供給数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、
を備えたことを特徴とするサーバ計算機保護装置。
【請求項２】
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、
一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するデータ供給数計測手段と、
前記データ要求数計測手段及びデータ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、
を備えたことを特徴とするサーバ計算機保護装置。
【請求項３】
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、
前記サーバ計算機から該サーバ計算機の処理状況に関する情報を受信する処理情報受信手段と

2

前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、
を備えたことを特徴とするサーバ計算機保護装置。
【請求項４】
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、
前記サーバ計算機から、前記データ要求受け付け手段で受け付けた前記所定のクライアント計算機のデータ要求に対する、該サーバ計算機が実行している処理の状況に関する情報を受信する処理情報受信手段と
前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、
を備えたことを特徴とするサーバ計算機保護装置。
【請求項５】
前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項１または請求項２に記載のサーバ計算機保護装置。
【請求項６】
前記サーバ計算機の負荷状態を値として記憶する負荷状態記憶手段をさらに備え、
前記サーバ負荷算出手段は、求めた前記サーバ計算機の負荷状態に応じて前記負荷状態記憶手段に記憶した値を増減し、
前記データ要求転送手段は、前記負荷状態記憶手段に記憶した値が高負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、低負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項１または請求項２に記載のサーバ計算機保護装置。
【請求項７】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項３または請求項４に記載のサーバ計算機保護装置。

【請求項８】

前記サーバ計算機の負荷状態を値として記憶する負荷状態記憶手段をさらに備え、
前記サーバ負荷算出手段は、求めた前記サーバ計算機の負荷状態に応じて前記負荷状態記憶手段に記憶した値を増減し、
前記データ要求転送手段は、前記負荷状態記憶手段に記憶した値が高負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、低負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項３または請求項４に記載のサーバ計算機保護装置。

【請求項９】

一定期間内に、前記サーバ計算機から前記クライアント計算機への応答に含まれるパケット量を計測する応答量計測手段をさらに備え、
前記サーバ負荷検出手段は、前記応答量計測手段が計測したパケット量が多いほどより負荷が高いと算出することを特徴とする請求項５または請求項６に記載のサーバ計算機保護装置。

【請求項１０】

前記サーバ計算機から前記クライアント計算機への応答があってから、該応答が再送されたことを検出する再応答検出手段をさらに備え、
前記サーバ負荷検出手段は、前記再応答検出手段が再送を検出すると、前記クライアント計算機のデータ要求による前記再送を行ったサーバ計算機の負荷がより高くなったと算出することを特徴とする請求項５または請求項６に記載のサーバ計算機保護装置。

【請求項１１】

前記クライアント計算機との接続が強制的に切断され、または通信状態に異常があることを検出する通信状態検出手段をさらに備え、
前記サーバ負荷算出手段は、前記通信状態検出手段が通信異常を検出すると、前記クライアント計算機に対する前記サーバ計算機の負荷がより高くなったと算出することを特徴とする請求項５または請求項６に記載のサーバ計算機保護装置。

【請求項１２】

前記クライアント計算機から新たな接続があったことを検出する接続検出手段をさらに備え、

前記サーバ負荷算出手段は、一定期間内に、前記接続検出手段が新たな接続を検出しない場合には、前記クライアント計算機に対する前記サーバ計算機の負荷がより低くなったと算出することを特徴とする請求項５または請求項６に記載のサーバ計算機保護装置。

【請求項１３】

前記サーバ負荷算出手段は、前記処理情報受信手段が直前に受信した情報と、前記データ要求受け付け手段が受け付けたデータ要求の処理を前記サーバ計算機が開始した後の、該処理の実行中に受信した情報から、該サーバ計算機の負荷の差が所定の値よりも大きく上昇したと判断したときは前記クライアント計算機に対する前記サーバ計算機の負荷が高くなったと算出することを特徴とする請求項７または請求項８に記載のサーバ計算機保護装置。

【請求項１４】

前記サーバ負荷算出手段は、前記処理情報受信手段が直前に受信した情報と、前記サーバ計算機が前記データ要求の処理を終了した直後に受信した情報から、前記直前に受信した情報と比べて、該サーバ計算機の負荷の差が所定の値よりも大きく低下したと判断したときは前記クライアント計算機に対する前記サーバ計算機の負荷が高いと算出することを特徴とする請求項７または請求項８に記載のサーバ計算機保護装置。

【請求項１５】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、
前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項１６】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項１７】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項１５または請求項１６に記載のサーバ計算機保護方法。

【請求項１８】

前記データ要求転送ステップは、求めた前記サーバ計算機の前記クライアント計算機に対する負荷状態に応じて、予め記憶した値を増減し、
前記記憶した値が高負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、低負荷を示すほど前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項１５または請求項１６に記載のサーバ計算機保護方法。

【請求項１９】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、
前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護プログラム。

【請求項２０】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項７に記載のサーバ計算機保護プログラム。

【請求項２１】

クライアント計算機からの要求に応じたデータを供給するサーバ計算機であって、
所定のデータ要求を処理して、該データ要求をしたクライアント計算機に供給するデータを作成するデータ処理手段と、
所定のクライアント計算機から送られてくるデータ要求を受け付けるデータ要求受け付け手段と、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、
一定期間内に、前記所定のクライアント計算機へ応答した数を計測するデータ供給数計測手段と、
前記データ要求数計測手段及びデータ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対する負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記データ処理手段へ転送するデータ要求の数の割合を変化させるデータ要求転送手段とを備え、
不特定のクライアント計算機からのDoS攻撃を受けたときに、正当なデータ要求を行っていた所定のクライアント計算機からのデータ要求、および正当なデータ要求を行っているにもかかわらず、DoS攻撃を行っていると判断された所定のクライアント計算機からのデータ要求が継続して処理されること特徴とするサーバ計算機。

【請求項２２】

クライアント計算機からの要求に応じたデータを供給するサーバ計算機であって、
所定のデータ要求を処理して、該データ要求をしたクライアント計算機に供給するデータを作成するデータ処理手段と、
所定のクライアント計算機から送られてくるデータ要求を受け付けるデータ要求受け付け手段と、
前記サーバ計算機から、前記データ要求受け付け手段で受け付けた前記所定のクライアント計算機のデータ要求に対する、該サーバ計算機が実行している処理の状況に関する情報を受信する処理情報受信手段と
前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた

前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記データ処理手段へ転送するデータ要求の数の割合を変化させるデータ要求転送手段とを備え、
不特定のクライアント計算機からのDoS攻撃を受けたときに、正当なデータ要求を行っていた所定のクライアント計算機からのデータ要求、および正当なデータ要求を行っているにもかかわらず、DoS攻撃を行っていると判断された所定のクライアント計算機からのデータ要求が継続して処理されること特徴とするサーバ計算機。

【請求項２３】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、
一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とするサーバ計算機保護装置を備えた請求項２１または請求項２２に記載のサーバ計算機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアントとなる計算機とサーバとなる計算機間のネットワークシステムに関し、特に、意図的にサーバ計算機の処理を妨害する不正なアクセスからサーバとなる計算機を保護するサーバ計算機保護装置に関する。

【０００２】

【従来の技術】

近年、インターネット等を利用し、不特定あるいは特定のクライアントとなる計算機をネットワーク経由でサーバとなる計算機に接続し、クライアントからの要求に応じてサーバからデータを供給することを目的とするクライアント・サーバシステムが広く使われている。

【０００３】

インターネット等のネットワークを流れるデータの形式として、宛先情報を付して伝送データを所定の大きさに再構成したパケットが一般に利用されている。パケットは、大まかに分けると、ヘッダとデータ本体とで構成されている。ヘッダには、このパケットの送り元である送信元の計算機を示すＩＰ(Internet Protocol)アドレスと、このパケットの宛先となる計算機のＩＰアドレスといったアドレス情報をもっている。

【０００４】

昨今、このようなネットワークに接続されたシステムに対し、システム的な障害を発生させることを目的としたネットワーク越しの攻撃が増加する傾向にある。たとえば、一つのクライアントから同時に大量のアクセス要求をサーバ計算機に対して行うことにより、攻撃対象となるサーバの稼動を妨げ実質的にサービスを不能にする攻

撃方法(以下、DoS攻撃(Denial of Service attack)と表記)がある。

【０００５】

この攻撃方法は、システム攻撃を意図しない正当なクライアントからのアクセスとの区別がつきにくいために、サーバ側で攻撃を回避することが極めて困難である。場合によっては複数のクライアントからこの攻撃を受けることもあり、これを特にDDoS攻撃(Distributed Denial of Service attack)と呼んでいる。

【０００６】

サーバへの要求がサーバの処理能力を超えるほど大量に送りつけられると、その要求毎に通信処理用の資源、たとえばメモリ領域や回線の帯域などが次々と確保されるためついには不足を来たし、妨害を意図していない正当なクライアントからの要求に対しサーバが応答できなくなるか、あるいは大きく滞ってしまうという結果を招く。

【０００７】

従来は、これらの攻撃を排除するためにサーバとネットワークの間にサーバ計算機保護装置を配置していた。このサーバ計算機保護装置は、複数回のアクセス要求が繰り返されたもののみを正当なアクセス要求として処理する、または既に正当なアクセスがあったクライアントからのアクセスを正当なアクセス要求として処理し、それ以外のアクセスについてはパケットを破棄するなどの処理を行っていた。

【０００８】

しかし、このような方法では、攻撃を意図するクライアントが同じような大量のアクセス要求を行う場合、攻撃を排除できないという問題点があった。

【０００９】

一方、上記問題を解決しても、たとえば特定のクライアントが大量のアクセス要求を行うとその通信行為がDoS攻撃であると判断されてしまうため、たとえそれが正当な要求であっても不正なアクセスとみなされる場合があった。DoS攻撃とみなされれば判断されたクライアントの接続は切断されてしまうため、そのクライアントで行っている業務に支障を来たす。

【００１０】

【特許文献１】特開２００２－１６６３３公報

【００１１】

【発明が解決しようとする課題】

本発明は、不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機を提供することを目的とする。

【００１２】

【課題を解決するための手段】
本発明にかかるサーバ計算機保護装置とすれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、
一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、
一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ供給数計測手段と、
前記データ供給数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、
を備えたことを特徴とするサーバ計算機保護装置
が提供される。または、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、
前記サーバ計算機から該サーバ計算機の処理状況に関する情報を受信する処理情報受信手段と
前記処理情報受信手段が受信した情報から、前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、
前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、
を備えたことを特徴とするサーバ計算機保護装置が提供される。
【００１３】
また本発明にかかるサーバ計算機保護方法によれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、
クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、
前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた

前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法
が提供される。
【００１４】
加えて、本発明にかかるサーバ計算機保護プログラムとすれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、
所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、
一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、
一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、
前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、
前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護プログラム
が提供される。
【００１５】
さらに、本発明にかかるサーバ計算機保護装置を備えたサーバ計算機が提供される。
【００１６】
【発明の実施の形態】
（第１の実施形態）
図１に第１の実施形態におけるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図１では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント１０１－１、１０１－２、１０１－３と、ネットワーク１０２およびサーバ保護装置１０３が存在する。また、クライアント１０１で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置１０３を介して受信し、さらにサーバ計算機保護装置１０３を介して送信する計算機であるサーバ１０４とからなる。クライアント１０１はサーバ１０４へ処理に必要なデータを要求し、サーバ１０４はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント１０１とサーバ１０４との通信は、すべてサーバ計算機保護装置１０３を介して行われる。
【００１７】

11

図２に第１の実施形態におけるサーバ計算機保護装置１０３の構成図の一例を示す。サーバ計算機保護装置１０３は、データ要求受け付け部２０１、データ要求転送部２０２、データ要求計測部２０３、データ供給数計測部２０４および応答確率算出部２０５からなる。

【００１８】

クライアント１０１はサーバ計算機保護装置１０３を介してサーバ１０４との接続を確立した後、処理に必要なデータをサーバ１０４に対して要求する。このときデータ要求受け付け部２０１によって、サーバ１０４に対する要求を受け付けるとともに、データ要求数計測部２０３によって受け付け中の要求の数を計測する。

【００１９】

データ要求受け付け部２０１によって受け付けられた要求は、データ要求転送部２０２によってサーバ１０４へと転送される。サーバ１０４はこの転送された要求に対するデータを、サーバ計算機保護装置１０３を介して、この要求を行ったクライアント１０１に向けて送信する。このときサーバ計算機保護装置１０３が備えるデータ供給数計測部２０４は、サーバ１０４のこの送信によって、受け付け済みの要求の完了数を計測する。つまりクライアント１０１に対してすべての応答が完了したときには、データ要求数計測部２０３で計測した受け付け中の要求数と、データ供給数計測部２０４で計測した完了済み要求数が一致することになる。

【００２０】

仮に、データ要求数計測部２０３で計測された受け付け中の要求数が、データ供給数計測部２０４で計測した完了済み要求数よりも多い場合を考える。受け付け中の要求数が完了済み要求数より多いということはすなわち受け付けた要求に対する処理について、サーバ１０４の処理が遅れている（処理が重い）ことを意味する。完了済み要求数よりも受け付け中の要求数が増加していけば行くほどサーバ１０４の応答は遅延し、ひいてはサーバ１０４が提供しているサービスがすべて停止してしまうことも考えられる。この状態はサーバ１０４がクライアント１０１からDoS攻撃を受けた状態と同じである。サーバ１０４の管理者はサーバ１０４の停止を回避するため、クライアント１０１からサーバ１０４へ送信される要求を速やかに停止させなければならない。

【００２１】

しかしながらクライアント１０１はあくまで正当なデータ要求を行っているだけであるとすれば、この決定によってクライアント１０１で稼動するアプリケーションの処理が中断あるいは処理そのものができないことになる。

【００２２】

上記したような不具合を緩和するために、応答確率算出部２０５は受け付け中の要求数と完了済み要求数の差を元に、応答確率を少なくとも指示を行う都度算出し、これをデータ要求転送部２０２に指示する。ここでいう応答確率とは、一定期間内に受け付けたクライアント１０１からのデータ要求の数に対して、サーバ１０４が一定期間内に応答したデータ応答数の比率をいう。データ要求転送部２０２は、この値が大きければ一定期間内に受け付けたデータ要求のうち一定期間内にサーバ１０４へ転送するデータ要求の数を増やし、逆に小さければ一定期間内にサーバ１０４へ転送するデータ要求の数を減らす。

12

【００２３】

一定期間内に転送される要求数を減らしたために、データ要求転送部２０２によって転送されなかったデータ要求は、データ要求受け付け部２０１から破棄される。あるいは破棄することなくデータ要求受け付け部２０１に保留するようにしてもよい。ただし破棄をせずデータ要求を保留する場合には、保留したデータ要求を、新たなデータ要求とは非同期に転送するための構成を必要とするが、本実施形態では説明しない。

【００２４】

応答確率算出部２０５は、受け付け中の要求数と完了済み要求数との差が少なくなるとサーバ１０４の負荷が軽いと判断して応答確率を高く算出し、また各要求数の差が大きくなるとサーバ１０４の負荷が高いと判断し応答確率を低く算出する。

【００２５】

上記のように構成すると、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【００２６】

なお、データ要求数計測部２０３の受け付け中の要求数とデータ供給数計測部２０４が計測する完了済み要求数のそれぞれの数は、たとえば前者を加算、後者を減算するようにして差分値のみを保持するようにしてもよい。結果的に両者の比較が可能な手段で蓄積されていれば足りる。

【００２７】

図３に第１の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【００２８】

サーバ計算機保護装置１０３を介してクライアント１０１からサーバ１０４への接続が確立された後、クライアント１０１からサーバ１０４に向けてデータ要求がされるのを待つ（Ｓ１）。データの要求がされたならばデータ要求数計測部２０３によって、応答確率算出部２０５が保持する受け付け中の要求数を１増加させる（Ｓ２）。

【００２９】

データ要求受け付け部２０１によって受け付けられたク

ライアント１０１からのデータ要求は、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断される（Ｓ３）。ステップＳ３の判断に際しては、未完了の受け付け中の要求数が使用される。

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほどサーバ１０４の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ１０４がデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００３０】

上記したような理由からステップＳ３の判定に、未完了の受け付け要求数を、サーバ１０４の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ１０４がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップＳ３では、この未完了の受け付け要求数に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００３１】

さらに以下に説明する基準も、応答確率算出部２０５が算出し、データ要求転送部２０２が転送するデータ要求の応答確率に反映することができる。

【００３２】

通信データにはデータ量を示す情報が付加されているため、データ供給数計測部２０４でサーバ１０４がクライアント１０１からのデータ要求に対するデータ応答のデータ量を計測することができる。応答するデータ量が多いということはサーバ１０４が応答データを作成するのに多くのコストを費やしていることを意味している。加えてこの通信に費やす時間も多くなり、通信回線の占有時間が長くなる。サーバ１０４の処理負荷及び通信回線の占有もまた、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００３３】

図３に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、このデータ応答のデータ量が考慮される。

【００３４】

ステップＳ３では、このデータ応答のデータ量に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。データ量がより少なければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００３５】

データ要求と、サーバ１０４が対応するデータ応答とはそれぞれ対応した順番号が付与されている。このためあるデータ応答がどのデータ要求のものかが特定することができる。

【００３６】

このとき、クライアント１０１からのあるデータ要求に対しサーバ１０４が応答したとする。その後、クライアント１０１からこのデータ応答に対する確認応答が所定時間得られなかったとすると、サーバ１０４は先のデータ応答がクライアント１０１に到達しなかったと判断して再送を試みる。データ供給数計測部２０４は、上述したように、再送したデータ応答はどのデータ要求の応答であるかが特定することができる。

【００３７】

この仕組みはサーバ１０４がクライアント１０１に対して確実に通信を行うための手段であるが、クライアント１０１が意図的に確認応答を返答しない場合も考えられる。するとサーバ１０４は際限なく再送を繰り返し、ひいては無用な処理負荷を伴い、同時に無用な再送により通信回線も占有してしまう。この場合もまたサーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００３８】

図３に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、このデータ応答の再送回数が考慮される。

【００３９】

ステップＳ３では、このデータ応答の再送回数に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。再送回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００４０】

データ要求受け付け部２０１は、サーバ１０４の代理としてクライアント１０１からのデータ要求を受け付ける。このとき、クライアント１０１が要求し、サーバ１０４と接続したコネクションが不当に切断されると、データ要求受け付け部２０１はこの不当な切断を検出することができる。不当な切断とは、例えば通信に使用するプロトコルに適合しない異常なコマンドの送出またはフローなどにより、正常な通信が維持できなくなったことを検出し切断されてしまうことをいう。またクライアン

ト１０１からの一方的な強制切断要求などを受けることも含まれる。

【００４１】

サーバ１０４は、異常なコマンドやフローまたは強制切断要求を受け取るとこれらは予期しないデータであることから通信資源のリカバリ処理を行わねばならなくなる。サーバ１０４内で稼動する更新アプリケーションがあった場合には、上記リカバリ処理の中でロールバックなどの更新取り消し処理が必要となることも考えられる。これらの処理はサーバ１０４に対し多大な負荷を与えることが多い。このような異常な通信が繰り返し行われるとサーバ１０４の負荷が上がり、サーバ１０４全体の処理効率が著しく低下する。この場合もまたサーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００４２】

図３に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、この異常な通信の回数が考慮される。

【００４３】

ステップＳ３では、この異常な通信の回数に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００４４】

上記のように、いくつかの判断基準を設けることにより効果的にDoS攻撃を防止することが可能となる。

【００４５】

応答確率算出部２０５の応答確率の算出に際して、この応答確率算出部２０５の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【００４６】

データ要求数計測部２０３、データ供給数計測部２０４及びデータ要求受け付け部２０１から取得した情報を基に応答確率算出部２０５はサーバ１０４の負荷を判断する。このとき、算出した値をそのままサーバ１０４の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【００４７】

例えば、各計測部から得られた値を総合して０から１０までの負荷レベルを示す値に変換していたものとする。各計測部から得られる値によっては０から１０まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【００４８】

そこで、各計測部から得られた値を総合して±２の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±２の範囲でしか変動しないため、応答確率記憶部が０から１０までの値を保持するものだとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【００４９】

仮に応答確率の変動があまりに急さに行われるとサーバ１０４にかかる負荷が一定せず、サーバ１０４が不安定になる場合がある。

【００５０】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント１０１からサーバ１０４に到達するデータ要求数の変動を緩和し、サーバ１０４を保護することができる。

【００５１】

このときサーバ１０４にクライアント１０１からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ１０４に転送する（Ｓ４）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部２０１から破棄し、再びクライアント１０１からの新たなデータ要求を待つ（Ｓ１）。

【００５２】

クライアント１０１からのデータ要求をサーバ１０４に転送したときには、次にこのデータ要求に対するサーバ１０４からの応答があるので、これをクライアント１０１に対して転送する（Ｓ５）。

【００５３】

そしてこの応答からデータ供給数計測部２０４によって完了済みの要求を計測し、応答確率算出部２０５が保持する受け付け中の要求数を１減少させる（Ｓ６）。　クライアント１０１からサーバ１０４への接続が確立されたままならば再び同様の動作フローを繰り返し、クライアント１０１からサーバ１０４に向けて新たなデータ要求がされるのを待つ（Ｓ１）。

【００５４】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【００５５】

（第２の実施形態）

図１に第２の実施形態における、サーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図１では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント１０１－１、１０１－２、１０１

－３と、ネットワーク１０２およびサーバ保護装置１０３が存在する。また、クライアント１０１で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置１０３を介して受信し、さらにサーバ計算機保護装置１０３を介して送信する計算機であるサーバ１０４とからなる。クライアント１０１はサーバ１０４へ処理に必要なデータを要求し、サーバ１０４はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント１０１とサーバ１０４との通信は、すべてサーバ計算機保護装置１０３を介して行われる。

【００５６】

図４に第２の実施形態におけるサーバ計算機保護装置１０３の構成図の一例を示す。サーバ計算機保護装置１０３は、データ要求受け付け部２０１、データ要求転送部２０２、データ要求計測部２０３、データ供給数計測部２０４および応答確率算出部２０５からなる。図２に示した第１の実施形態におけるサーバ計算機保護装置１０３との相違は、データ要求数計測部２０３及び応答確率算出部２０５を複数備えていることである。これら複数の各計測部は、複数あるクライアント１０１（たとえばクライアント１０１－１、１０１－２、１０１－３）のそれぞれから送信されるデータ要求の転送を、それぞれのクライアントごとに処理するために構成されている。クライアントごとの処理を行うためには、処理すべき要求がどのクライアントが発信したものであるかの判別が必要となる。この判別は、各クライアントから送信されるデータ要求に含まれるパケットのヘッダ情報の送信元を示すＩＰアドレスを参照することにより可能である。同様にサーバが行うサーバ応答の宛先のクライアントも、サーバ応答に含まれるパケットのヘッダ情報の宛先を示すＩＰアドレスを参照することにより判別可能である。

【００５７】

各構成要素の動作は第１の実施形態のものと同じである。

【００５８】

図５に第２の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【００５９】

サーバ計算機保護装置１０３を介してクライアント１０１からサーバ１０４への接続が確立され、そのクライアント１０１にデータ要求数計測部２０３と応答確率算出部２０５の組が割り当てられた後、クライアント１０１からサーバ１０４に向けてデータ要求がされるのを待つ（Ｓ１）。データの要求がされたならばそのデータ要求を行ったクライアント１０１に割り当てられているデータ要求数計測部２０３によって、その組となっている応答確率算出部２０５が保持する受け付け中の要求数を１増加させる（Ｓ７）。

【００６０】

データ要求受け付け部２０１によって受け付けられた所定のクライアント１０１からのデータ要求は、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断される（Ｓ３）。ステップＳ３の判断に際しては、未完了の受け付け中の要求数が使用される。

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほど所定のクライアント１０１によるサーバ１０４の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ１０４が所定のクライアント１０１によるデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００６１】

上記したような理由からステップＳ３の判定に、未完了の受け付け要求数を、サーバ１０４の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ１０４がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップＳ３では、この未完了の受け付け要求数に応じて所定のクライアント１０１からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００６２】

さらに以下に説明する基準も、応答確率算出部２０５が算出し、データ要求転送部２０２が転送するデータ要求の応答確率に反映することができる。

【００６３】

通信データにはデータ量を示す情報が付加されているため、データ供給数計測部２０４でサーバ１０４がクライアント１０１からのデータ要求に対するデータ応答のデータ量を計測することができる。応答するデータ量が多いということはサーバ１０４が応答データを作成するのに多くのコストを費やしていることを意味している。加えてこの通信に費やす時間も多くなり、通信回線の占有時間が長くなる。サーバ１０４の処理負荷及び通信回線の占有もまた、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００６４】

図３に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送し

ても良いものかどうかが判断されるステップＳ３の判断に際しては、このデータ応答のデータ量が考慮される。

【００６５】

ステップＳ３では、このデータ応答のデータ量に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。データ量がより少なければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００６６】

データ要求と、サーバ１０４が対応するデータ応答とはそれぞれ対応した順番号が付与されている。このためあるデータ応答がどのデータ要求のものかが特定することができる。

【００６７】

このとき、クライアント１０１からのあるデータ要求に対しサーバ１０４が応答したとする。その後、クライアント１０１からこのデータ応答に対する確認応答が所定時間得られなかったとすると、サーバ１０４は先のデータ応答がクライアント１０１に到達しなかったと判断して再送を試みる。データ供給数計測部２０４は、上述したように、再送したデータ応答はどのデータ要求の応答であるかが特定することができる。

【００６８】

この仕組みはサーバ１０４がクライアント１０１に対して確実に通信を行うための手段であるが、クライアント１０１が意図的に確認応答を返答しない場合も考えられる。するとサーバ１０４は際限なく再送を繰り返し、ひいては無用な処理負荷を伴い、同時に無用な再送により通信回線も占有してしまう。この場合もまたサーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００６９】

図３に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、このデータ応答の再送回数が考慮される。

【００７０】

ステップＳ３では、このデータ応答の再送回数に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。再送回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００７１】

データ要求受け付け部２０１は、サーバ１０４の代理としてクライアント１０１からのデータ要求を受け付ける。このとき、クライアント１０１が要求し、サーバ１０４と接続したコネクションが不当に切断されると、データ要求受け付け部２０１はこの不当な切断を検出することができる。不当な切断とは、例えば通信に使用するプロトコルに適合しない異常なコマンドの送出またはフローなどにより、正常な通信が維持できなくなったことを検出し切断されてしまうことをいう。またクライアント１０１からの一方的な強制切断要求などを受けることも含まれる。

【００７２】

サーバ１０４は、異常なコマンドやフローまたは強制切断要求を受け取るとこれらは予期しないデータであることから通信資源のリカバリ処理を行わねばならなくなる。サーバ１０４内で稼動する更新アプリケーションがあった場合には、上記リカバリ処理の中でロールバックなどの更新取り消し処理が必要となることも考えられる。これらの処理はサーバ１０４に対し多大な負荷を与えることが多い。このような異常な通信が繰り返し行われるとサーバ１０４の負荷が上がり、サーバ１０４全体の処理効率が著しく低下する。この場合もまたサーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００７３】

図３に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、この異常な通信の回数が考慮される。

【００７４】

ステップＳ３では、この異常な通信の回数に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。回数が多ければ多いほどDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００７５】

上記のように、いくつかの判断基準を設けることにより効果的にDoS攻撃を防止することが可能となる。

【００７６】

応答確率算出部２０５の応答確率の算出に際して、この応答確率算出部２０５の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【００７７】

データ要求数計測部２０３、データ供給数計測部２０４及びデータ要求受け付け部２０１から取得した情報を基に応答確率算出部２０５は各クライアントが掛けているサーバ１０４の負荷を判断する。このとき、算出した値をそのままサーバ１０４の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【００７８】

例えば、各計測部から得られた値を総合して０から１０までの負荷レベルを示す値に変換していたものとする。

各計測部から得られる値によっては０から１０まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【００７９】

そこで、各計測部から得られた値を総合して±２の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±２の範囲でしか変動しないため、応答確率記憶部が０から１０までの値を保持するものだとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【００８０】

仮に応答確率の変動があまりに急さに行われるとサーバ１０４にかかる負荷が一定せず、サーバ１０４が不安定になる場合がある。

【００８１】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント１０１からサーバ１０４に到達するデータ要求数の変動を緩和し、サーバ１０４を保護することができる。

【００８２】

このときサーバ１０４に所定のクライアント１０１からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ１０４に転送する（Ｓ８）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部２０１から破棄し、再び所定のクライアント１０１からの新たなデータ要求を待つ（Ｓ１）。

【００８３】

所定のクライアント１０１からのデータ要求をサーバ１０４に転送したときには、次にこのデータ要求に対するサーバ１０４からの応答があるので、これを所定のクライアント１０１に対して転送する（Ｓ５）。

【００８４】

そしてこの応答からデータ供給数計測部２０４によって完了済みの要求を計測し、所定のクライアント１０１に割り当てられた応答確率算出部２０５が保持する受け付け中の要求数を１減少させる（Ｓ９）。　所定のクライアント１０１からサーバ１０４への接続が確立されたままならば再び同様の動作フローを繰り返し、所定のクライアント１０１からサーバ１０４に向けて新たなデータ要求がされるのを待つ（Ｓ１）。

【００８５】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントを停止させることなく、またクライアントごとのきめ細かなサーバ計算機保護のための制御を可能としたサーバ計算機保護装置とすることができる。

【００８６】

（第３の実施形態）

図１に第３の実施形態におけるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図１では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント１０１－１、１０１－２、１０１－３と、ネットワーク１０２およびサーバ保護装置１０３が存在する。また、クライアント１０１で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置１０３を介して受信し、さらにサーバ計算機保護装置１０３を介して送信する計算機であるサーバ１０４とからなる。クライアント１０１はサーバ１０４へ処理に必要なデータを要求し、サーバ１０４はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント１０１とサーバ１０４との通信は、すべてサーバ計算機保護装置１０３を介して行われる。

【００８７】

図６に第３の実施形態におけるサーバ計算機保護装置１０３の構成図の一例を示す。サーバ計算機保護装置１０３は、データ要求受け付け部２０１、データ要求転送部２０２、応答確率算出部２０５および処理状況受信部２０６からなる。

【００８８】

クライアント１０１はサーバ計算機保護装置１０３を介してサーバ１０４との接続を確立した後、処理に必要なデータをサーバ１０４に対して要求する。このときデータ要求受け付け部２０１によって、サーバ１０４に対する要求を受け付ける。

【００８９】

データ要求受け付け部２０１によって受け付けられた要求は、データ要求転送部２０２によってサーバ１０４へと転送される。サーバ１０４はこの転送された要求に対するデータを、サーバ計算機保護装置１０３を介して、この要求を行ったクライアント１０１に向けて送信する。

【００９０】

処理状況受信部２０６はサーバ１０４から、サーバ１０４自身の処理状況についての情報を受信する。具体的には、たとえばサーバ１０４の送信時の負荷状況などである。サーバ１０４が通知する情報にはデータ要求受け付け部２０１が受け付けたデータ要求と、サーバ１０４が処理している状況あるいは処理した結果とが結び付けられて格納されていても良い。この場合はたとえば、あるデータ要求と、このデータ要求を処理するために起動したアプリケーションがサーバ１０４に対して掛けた負荷とが関連することが分かるような情報である。

【００９１】

所定の時間間隔あるいは任意のタイミングで所得した、サーバ１０４から得られた処理状況情報を分析すると、

クライアント１０１が要求したデータ要求とサーバ１０４の負荷状況との関係が分かる。たとえば、クライアント１０１からあるデータ要求があった後にサーバ１０４の負荷が急激に変動するような特徴が発見できる。もしもサーバ１０４の負荷を急激に上げるようなデータ要求を立て続けに行うクライアント１０１があった場合には、サーバ１０４の処理能力を著しく消費する。ひいてはサーバ１０４が提供しているサービスがすべて停止してしまうことも考えられる。この状態はサーバ１０４がクライアント１０１からDoS攻撃を受けた状態と同じである。サーバ１０４の管理者はサーバ１０４の停止を回避するため、クライアント１０１からサーバ１０４へ送信される要求を速やかに停止させなければならない。

【００９２】

しかしながらクライアント１０１はあくまで正当なデータ要求を行っているだけであるとすれば、この決定によってクライアント１０１で稼動するアプリケーションの処理が中断あるいは処理そのものができないことになる。

【００９３】

上記したような不具合を緩和するために、応答確率算出部２０５は処理状況情報を元に、応答確率を少なくともサーバ１０４から情報を取得する都度算出し、これをデータ要求転送部２０２に指示する。ここでいう応答確率とは、一定期間内に受け付けたクライアント１０１からのデータ要求の数に対して、サーバ１０４が一定期間内に応答したデータ応答数の比率をいう。データ要求転送部２０２は、この値が大きければ一定期間内に受け付けたデータ要求のうち一定期間内にサーバ１０４へ転送するデータ要求の数を増やし、逆に小さければ一定期間内にサーバ１０４へ転送するデータ要求の数を減らす。

【００９４】

一定期間内に転送される要求数を減らしたために、データ要求転送部２０２によって転送されなかったデータ要求は、データ要求受け付け部２０１から破棄される。あるいは破棄することなくデータ要求受け付け部２０１に保留するようにしてもよい。ただし破棄をせずデータ要求を保留する場合には、保留したデータ要求を、新たなデータ要求とは非同期に転送するための構成を必要とするが、本実施形態では説明しない。

【００９５】

応答確率算出部２０５は、サーバ１０４から所得した処理状況情報からサーバ１０４の負荷が軽いと判断すると応答確率を高く算出し、またサーバ１０４の負荷が高いと判断すれば応答確率を低く算出する。

【００９６】

上記のように構成すると、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【００９７】

図７に第３の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【００９８】

図７（A）に示すフローは、サーバ１０４から処理状況情報を取得するためのものである。一方、図７（B）はクライアント１０１からデータ要求を受け付け、サーバ１０４に受け渡すフローを示している。これら二つのフローはそれぞれ非同期に処理される。

【００９９】

まず図７（A）について説明する。処理状況受信部２０６は、サーバ１０４から、このサーバが行っている処理の状況についての情報を取得すべく、この情報が送信されるのを待つ（Ｓ１０）。情報が正常に所得できたかどうかを判断し（Ｓ１１）、正常に取得できた場合には処理状況受信部２０６はこのサーバ１０４についての処理負荷を確定する（Ｓ１２）。この処理はサーバ１０４から処理状況情報を取得する都度実行し、サーバ１０４の処理負荷の状況をリアルタイムに確定する。

【０１００】

ステップＳ１１にて処理状況情報が取得できなかった場合は、再びこの情報が送信されるのを待つ（Ｓ１０）。

【０１０１】

次に図７（Ｂ）について説明する。

【０１０２】

サーバ計算機保護装置１０３を介してクライアント１０１からサーバ１０４への接続が確立された後、クライアント１０１からサーバ１０４に向けてデータ要求がされるのを待つ（Ｓ１）。

【０１０３】

データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求は、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断される（Ｓ３）。ステップＳ３の判断に際しては、処理状況受信部２０６が確定したサーバ１０４についての処理負荷が使用される。

負荷が低ければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により高ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【０１０４】

さらに以下に説明する基準も、応答確率算出部２０５が算出し、データ要求転送部２０２が転送するデータ要求の応答確率に反映することができる。

【０１０５】

サーバ１０４の処理状況情報を取りつづけていると、データ要求とサーバ１０４の負荷に特徴を見つけることができる場合がある。たとえば、データ要求受け付け部２０１が受け付け、データ要求転送部２０２がデータ要求

を転送した後に、決まってサーバ１０４の処理が急激に上昇するような場合である。
このような処理負荷が急激に上がるような傾向が見つかると、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【０１０６】
図７に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、この処理負荷が急激に上がる傾向があるかどうかが考慮される。

【０１０７】
ステップＳ３では、負荷のかかり方の傾向を判断しクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。負荷が急激に上がる傾向があるならばDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【０１０８】
逆に、クライアント１０１からのデータ要求が無くなったとたん、サーバ１０４の負荷が急激に低下する場合もある。このような処理負荷が急激に下がるような傾向が見つかると、サーバ１０４はDoS攻撃を受けていた可能性が高いと判断できる。

【０１０９】
図７に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、この処理負荷が急激に下がる傾向があるかどうかも考慮される。

【０１１０】
ステップＳ３では、負荷のかかり方の傾向を判断しクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。負荷が急激に下がる傾向があるならばDoS攻撃を受けていた可能性があるので新たなデータ要求は安易に受け付けず破棄すべきと判断する。

【０１１１】
応答確率算出部２０５の応答確率の算出に際して、この応答確率算出部２０５の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【０１１２】
処理状況受信部２０６が受信した、サーバ１０４の処理状況情報を基に応答確率算出部２０５はサーバ１０４の負荷を判断する。このとき、算出した値をそのままサーバ１０４の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【０１１３】
例えば、各計測部から得られた値を総合して０から１０までの負荷レベルを示す値に変換していたものとする。各計測部から得られる値によっては０から１０まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【０１１４】
そこで、各計測部から得られた値を総合して±２の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±２の範囲でしか変動しないため、応答確率記憶部が０から１０までの値を保持するものだとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【０１１５】
仮に応答確率の変動があまりに急さに行われるとサーバ１０４にかかる負荷が一定せず、サーバ１０４が不安定になる場合がある。

【０１１６】
前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント１０１からサーバ１０４に到達するデータ要求数の変動を緩和し、サーバ１０４を保護することができる。

【０１１７】
このときサーバ１０４にクライアント１０１からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ１０４に転送する（Ｓ４）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部２０１から破棄し、再びクライアント１０１からの新たなデータ要求を待つ（Ｓ１）。

【０１１８】
クライアント１０１からのデータ要求をサーバ１０４に転送したときには、次にこのデータ要求に対するサーバ１０４からの応答があるので、これをクライアント１０１に対して転送する（Ｓ５）。
クライアント１０１からサーバ１０４への接続が確立されたままならば再び同様の動作フローを繰り返し、クライアント１０１からサーバ１０４に向けて新たなデータ要求がされるのを待つ（Ｓ１）。

【０１１９】
このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【０１２０】
（第４の実施形態）
図１に第４の実施形態における、サーバ計算機保護装置

が適用されるネットワーク構成図の一例を示す。図１では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント１０１－１、１０１－２、１０１－３と、ネットワーク１０２およびサーバ保護装置１０３が存在する。また、クライアント１０１で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置１０３を介して受信し、さらにサーバ計算機保護装置１０３を介して送信する計算機であるサーバ１０４とからなる。クライアント１０１はサーバ１０４へ処理に必要なデータを要求し、サーバ１０４はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント１０１とサーバ１０４との通信は、すべてサーバ計算機保護装置１０３を介して行われる。

【０１２１】

図８に第４の実施形態におけるサーバ計算機保護装置１０３の構成図の一例を示す。サーバ計算機保護装置１０３は、データ要求受け付け部２０１、データ要求転送部２０２、応答確率算出部２０５及び処理状況受信部２０６からなる。図６に示した第３の実施形態におけるサーバ計算機保護装置１０３との相違は、応答確率算出部２０５を複数備えていることである。これら複数の各計測部は、複数あるクライアント１０１（たとえばクライアント１０１－１、１０１－２、１０１－３）のそれぞれから送信されるデータ要求の転送を、それぞれのクライアントごとに処理するために構成されている。クライアントごとの処理を行うためには、処理すべき要求がどのクライアントが発信したものであるかの判別が必要となる。この判別は、各クライアントから送信されるデータ要求に含まれるパケットのヘッダ情報の送信元を示すＩＰアドレスを参照することにより可能である。同様にサーバが行うサーバ応答の宛先のクライアントも、サーバ応答に含まれるパケットのヘッダ情報の宛先を示すＩＰアドレスを参照することにより判別可能である。

【０１２２】

各構成要素の動作は第３の実施形態のものと同じである。

【０１２３】

図９に第４の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【０１２４】

図９（A）に示すフローは、サーバ１０４から処理状況情報を取得するためのものである。一方、図９（B）はクライアント１０１からデータ要求を受け付け、サーバ１０４に受け渡すフローを示している。これら二つのフローはそれぞれ非同期に処理される。

【０１２５】

まず図９（A）について説明する。処理状況受信部２０６は、サーバ１０４から、このサーバが行っている処理の状況についての情報を取得すべく、この情報が送信されるのを待つ（Ｓ１０）。情報が正常に所得できたかどうかを判断し（Ｓ１１）、正常に取得できた場合には処理状況受信部２０６はこのサーバ１０４に各クライアントが掛けている処理負荷をクライアントごとに確定する（Ｓ１３）。この処理はサーバ１０４から処理状況情報を取得する都度実行し、各クライアントが掛けているサーバ１０４の処理負荷の状況をリアルタイムに確定する。

【０１２６】

ステップＳ１１にて処理状況情報が取得できなかった場合は、再びこの情報が送信されるのを待つ（Ｓ１０）。

【０１２７】

次に図７（Ｂ）について説明する。

【０１２８】

サーバ計算機保護装置１０３を介してクライアント１０１からサーバ１０４への接続が確立され、そのクライアント１０１に応答確率算出部２０５が割り当てられた後、クライアント１０１からサーバ１０４に向けてデータ要求がされるのを待つ（Ｓ１）。

【０１２９】

データ要求受け付け部２０１によって受け付けられた所定のクライアント１０１からのデータ要求は、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断される（Ｓ３）。ステップＳ３の判断に際しては、処理状況受信部２０６が確定したサーバ１０４についての処理負荷が使用される。

負荷が低ければ所定のクライアントについてサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆に高ければそのクライアントからDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【０１３０】

さらに以下に説明する基準も、応答確率算出部２０５が算出し、データ要求転送部２０２が転送するデータ要求の応答確率に反映することができる。

【０１３１】

サーバ１０４の処理状況情報を取りつづけていると、各クライアントからのデータ要求とサーバ１０４の負荷に特徴を見つけることができる場合がある。たとえば、データ要求受け付け部２０１が受け付け、データ要求転送部２０２がデータ要求を転送した後に、決まってサーバ１０４の処理が急激に上昇するような場合である。

所定のクライアントについて、このような処理負荷が急激に上がるような傾向が見つかると、サーバ１０４はこのクライアントからDoS攻撃を受けている可能性が高いと判断できる。

【０１３２】

図９に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送し

ても良いものかどうかが判断されるステップＳ３の判断に際しては、この処理負荷が急激に上がる傾向があるかどうかが考慮される。

【０１３３】

ステップＳ３では、負荷のかかり方の傾向を判断しクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。所定のクライアントについて負荷が急激に上がる傾向があるならばそのクライアントからDoS攻撃を受けている可能性があるので、そのクライアントからの新たなデータ要求を破棄すべきと判断する。

【０１３４】

逆に、クライアント１０１からのデータ要求が無くなったとたん、サーバ１０４の負荷が急激に低下する場合もある。所定のクライアントについて、このような処理負荷が急激に下がるような傾向が見つかると、サーバ１０４はそのクライアントからDoS攻撃を受けていた可能性が高いと判断できる。

【０１３５】

図９に示した、データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求が、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断されるステップＳ３の判断に際しては、この処理負荷が急激に下がる傾向があるかどうかも考慮される。

【０１３６】

ステップＳ３では、負荷のかかり方の傾向を判断しクライアント１０１からの新たなデータ要求を転送しても良いかどうかも判断材料とする。負荷が急激に下がる傾向があるならばそのクライアントからDoS攻撃を受けていた可能性があるので、そのクライアントからの新たなデータ要求は安易に受け付けず破棄すべきと判断する。

【０１３７】

応答確率算出部２０５の応答確率の算出に際して、この応答確率算出部２０５の中に応答確率記憶部を持たせ、これが記憶する値を下記に示すように考慮するようにしても良い。

【０１３８】

処理状況受信部２０６が受信した、サーバ１０４の処理状況情報を基に応答確率算出部２０５は各クライアントが掛けているサーバ１０４の負荷を判断する。このとき、算出した値をそのままサーバ１０４の負荷状況に換算して判断するのではなく、この算出した値を前出の応答確率記憶部が記憶する値から相殺するようにする。

【０１３９】

例えば、各計測部から得られた値を総合して０から１０までの負荷レベルを示す値に変換していたものとする。各計測部から得られる値によっては０から１０まで劇的に変化する可能性があり、算出すべき応答確率が大きく変動することが予想される。

【０１４０】

そこで、各計測部から得られた値を総合して±２の範囲に収まるような値に変換する。次に、総合して得られたこの値を応答確率記憶部に記憶された値に加算する。すると、値の変化は一回の計測で±２の範囲でしか変動しないため、応答確率記憶部が０から１０までの値を保持するものだとすれば、先の例のように応答確率が大きく変動することを抑制することができる。

【０１４１】

仮に応答確率の変動があまりに急さに行われるとサーバ１０４にかかる負荷が一定せず、サーバ１０４が不安定になる場合がある。

【０１４２】

前出の応答確率記憶部が保持する値の範囲と各計測部から得られる値を総合した値の範囲を適切に決定することにより、クライアント１０１からサーバ１０４に到達するデータ要求数の変動を緩和し、サーバ１０４を保護することができる。

【０１４３】

このときサーバ１０４に所定のクライアント１０１からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ１０４に転送する（Ｓ８）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部２０１から破棄し、再び所定のクライアント１０１からの新たなデータ要求を待つ（Ｓ１）。

【０１４４】

所定のクライアント１０１からのデータ要求をサーバ１０４に転送したときには、次にこのデータ要求に対するサーバ１０４からの応答があるので、これを所定のクライアント１０１に対して転送する（Ｓ５）。

【０１４５】

所定のクライアント１０１からサーバ１０４への接続が確立されたままならば再び同様の動作フローを繰り返し、所定のクライアント１０１からサーバ１０４に向けて新たなデータ要求がされるのを待つ（Ｓ１）。

【０１４６】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントを停止させることなく、またクライアントごとのきめ細かなサーバ計算機保護のための制御を可能としたサーバ計算機保護装置とすることができる。

【０１４７】

（各実施形態における変形例）

各実施形態の変形例として、サーバ１０４に本実施形態にかかるサーバ計算機保護装置１０３の構成を組み込んだサーバ１０４とすることができる。このように構成するとクライアント１０１からのデータ要求を処理するサーバ１０４と、このサーバ１０４を不特定のクライアン

31

ト１０１からのDoS攻撃から保護する目的で設けるサーバ計算機保護装置１０３とを分離して個別に構築する必要がない。よってサーバ計算機保護装置１０３とサーバ１０４との通信をネットワーク等を介して行う必要もなくなり、代理応答の通信に要していた時間を排除することができる。また複数の筐体により構成したサーバ計算機保護装置１０３によって保護されたサーバ１０４の場合と比較して、同様の機能を１つの筐体で提供できる可能性があり、この場合には設置に必要なスペースを削減することができる。

【０１４８】

【発明の効果】

不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置とすることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態にかかるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す図である。

【図２】本発明の第１の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図３】本発明の第１の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

32

【図４】本発明の第２の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図５】本発明の第２の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

【図６】本発明の第３の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図７】本発明の第３の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

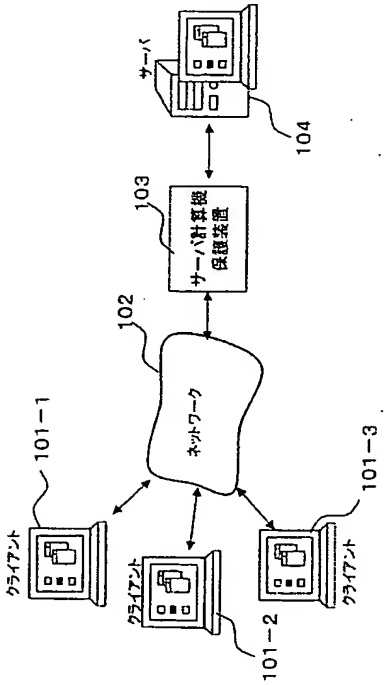
【図８】本発明の第４の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図９】本発明の第４の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

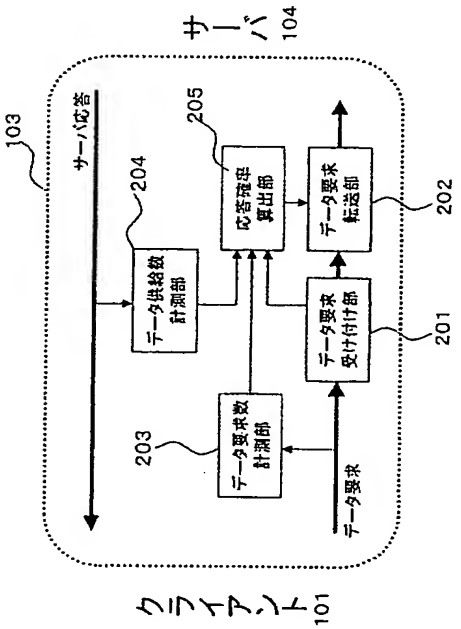
【符号の説明】

１０１－１	・・・	クライアント
１０１－２	・・・	クライアント
１０１－３	・・・	クライアント
１０２	・・・	ネットワーク
１０３	・・・	サーバ計算機保護装置
１０４	・・・	サーバ
２０１	・・・	データ要求受け付け部
２０２	・・・	データ要求転送部
２０３	・・・	データ要求数計測部
２０４	・・・	データ供給数計測部
２０５	・・・	応答確率算出部
２０６	・・・	処理状況受信部

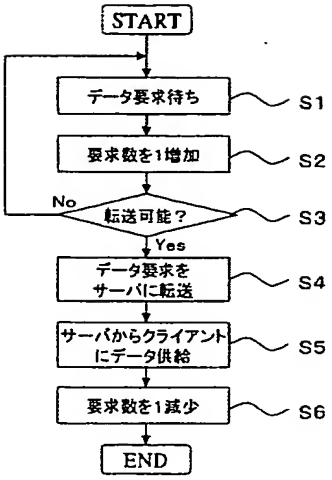
【図１】



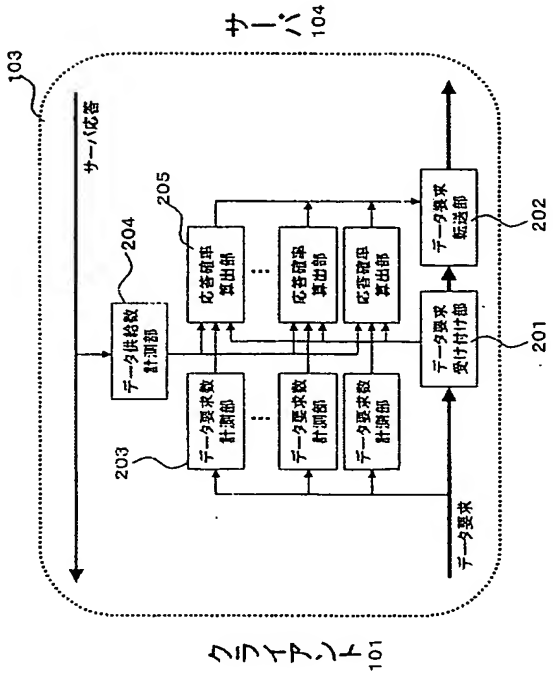
【図２】



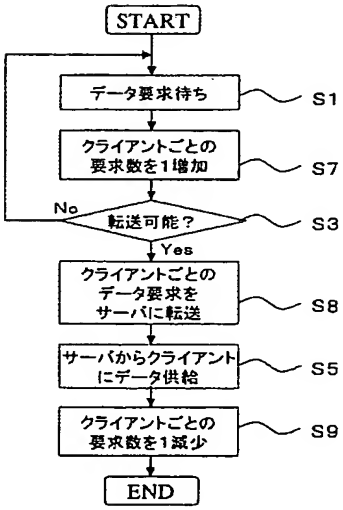
【図３】


START
データ要求待ち
S1
要求数を1増加
S2
No
転送可能？
S3
Yes
データ要求を
サーバに転送
S4
サーバからクライアント
にデータ供給
S5
要求数を1減少
S6
END

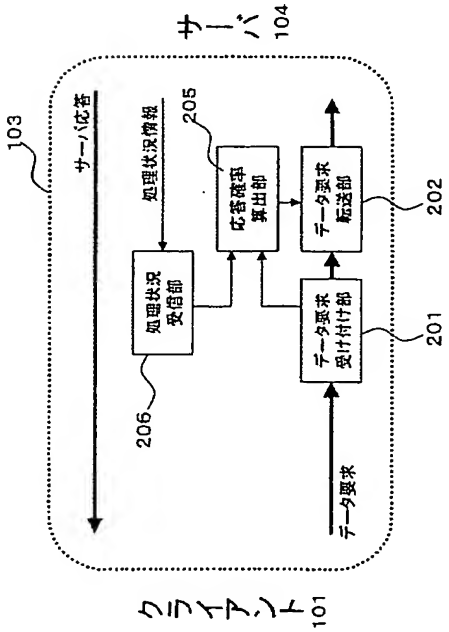
【図４】


サーバ
104
103
サーバ応答
204
205
データ供給数
計測部
応答確率
算出部
データ要求
転送部
202
データ要求
受け付け部
201
203
データ要求数
計測部
データ要求
クライアント
101

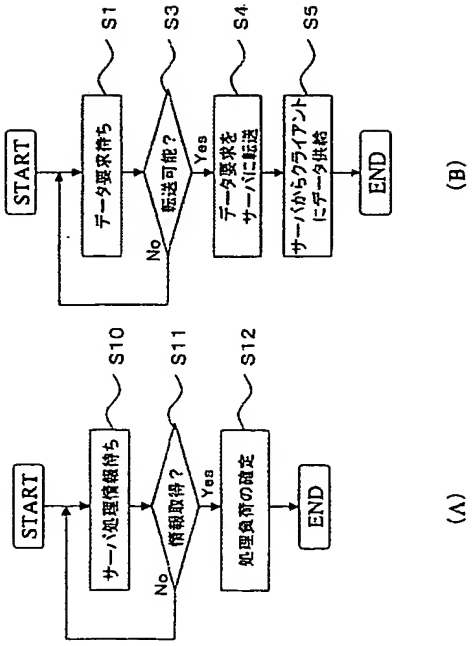
【図５】


START
データ要求待ち
S1
クライアントごとの
要求数を1増加
S7
No
転送可能？
S3
Yes
クライアントごとの
データ要求を
サーバに転送
S8
サーバからクライアント
にデータ供給
S5
クライアントごとの
要求数を1減少
S9
END

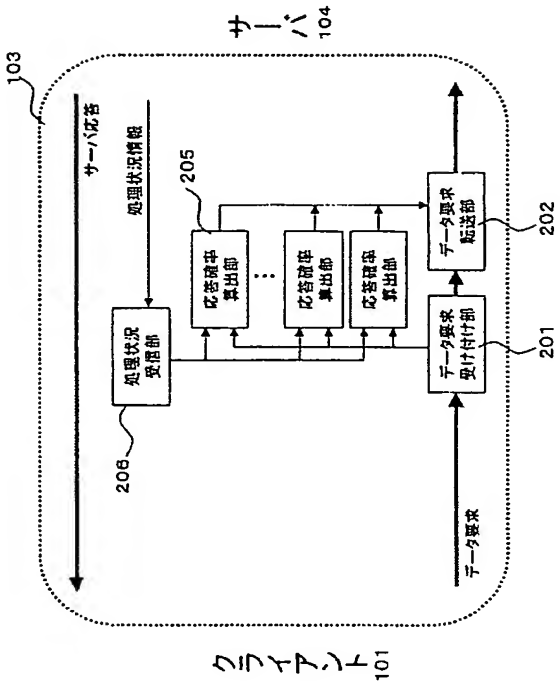
【図６】


サーバ
104
103
サーバ応答
処理状況情報
205
応答確率
算出部
データ要求
転送部
202
処理状況
受信部
206
データ要求
受け付け部
201
データ要求
クライアント
101

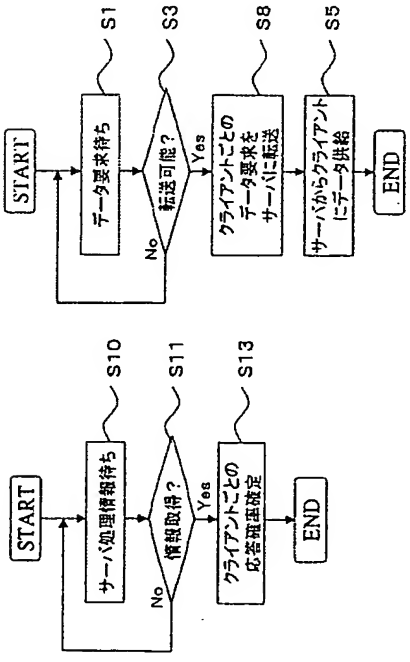
【図７】


START
データ要求待ち
S1
転送可能？
S3
No
Yes
データ要求をサーバに転送
S4
サーバからクライアントにデータ供給
S5
END
(B)
START
サーバ処理情報待ち
S10
情報取得？
S11
No
Yes
処理負荷の確定
S12
END
(A)

【図８】


サーバ
104
103
サーバ応答
処理状況情報
205
処理状況受信部
206
応答時間算出部
応答能率算出部
応答確率算出部
データ要求受け付け部
201
データ要求転送部
202
データ要求
クライアント
101

【図９】


START
データ要求待ち
S1
転送可能？
S3
No
Yes
クライアントごとのデータ要求をサーバに転送
S8
サーバからクライアントにデータ供給
S5
END
(B)
START
サーバ処理情報待ち
S10
情報取得？
S11
No
Yes
クライアントごとの応答確率確定
S13
END
(A)